ІНФОРМАТИКА

Основні ненавмисні й навмисні штучні загрози

За навчальною програмою 2018 року

Урок 3

Розділ 1
§ 3

Основні ненавмисні й навмисні штучні загрози

Класифікація загроз залежно від обсягів завданих збитків

Нешкідливі

- *Не завдають збитків*

Шкідливі

- *Завдають значних збитків*

Дуже шкідливі

- *Завдають критичних збитків*

Загрози інформації залежать від:

- ***характеристик обчислювальної системи,***
- ***фізичного середовища,***
- ***персоналу,***
- ***оброблюваної інформації.***

Розділ 1
§ 3

Класифікація загроз інформаційній безпеці

Залежно від результату шкідливих дій, загрози інформаційній безпеці можна поділити на такі види:

отримання доступу до секретних або конфіденційних даних;

порушення або повне припинення роботи комп'ютерної інформаційної системи;

отримання доступу до керування роботою комп'ютерної інформаційної системи.

Розділ 1
§ 3

Класифікація загроз інформаційній безпеці

Розглядають й інші класифікації загроз:

За метою	*За місцем виникнення*	*За походженням*
зловмисні, випадкові	*зовнішні, внутрішні*	*природні, техногенні, зумовлені людиною*

Розділ 1
§ 3

Класифікація загроз інформаційній безпеці

Перелік основних загроз інформаційній безпеці

- Знищення та спотворення даних
- Отримання доступу до секретних і конфіденційних даних
- Пошкодження пристроїв інформаційної системи
- Отримання прав на виконання дій, що передбачені тільки для окремих керівних осіб
- Отримання доступу до здійснення фінансових операцій замість власників рахунків
- Отримання повного доступу до керування інформаційною системою

Розділ 1
§ 3

Основні ненавмисні й навмисні штучні загрози

Загрози інформаційні безпеці

Природні (об’єктивні)	**Штучні** (суб’єктивні) - викликані впливом на інформаційну сферу людини	
	Ненавмисні (випадкові)	**Навмисні** (умисні)
викликані впливом на інформаційне середовище об’єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини	помилки програмного забезпечення, персоналу, збої в роботі систем, відмови обчислювальної та комунікаційної техніки	неправомірний доступ до інформації, розробка спеціального програмного забезпечення, використовуваного для здійснення неправомірного доступу, розробка та поширення вірусних програм і т.д.

Розділ 1
§ 3

Основні ненавмисні й навмисні штучні загрози

Ненавмисні штучні загрози:

- *ненавмисні дії, що призводять до часткової або повної відмови системи або руйнування апаратних, програмних, інформаційних ресурсів системи;*
- *ненавмисне псування носіїв інформації;*
- *зараження комп'ютера вірусами;*
- *необережні дії, що призводять до розголошення конфіденційної інформації або роблять її загальнодоступною;*
- *розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, перепусток тощо).*

Розділ 1
§ 3

Основні ненавмисні й навмисні штучні загрози

Навмисні штучні загрози:

- *фізичне руйнування системи (вибух, підпал тощо) або виведення з ладу найбільш важливих компонентів системи (пристроїв, носіїв важливої інформації, осіб з персоналу і т. д.);*
- *відключення або виведення з ладу важливих підсистем (електроживлення, охолодження та вентиляції, ліній зв'язку тощо);*
- *вербування (підкуп, шантаж тощо) персоналу або окремих користувачів, що мають певні повноваження;*

Розділ 1
§ 3

Основні ненавмисні й навмисні штучні загрози

(Продовження...) Ненавмисні штучні загрози:

- несанкціоноване копіювання носіїв інформації;
- зчитування залишкової інформації з оперативної пам’яті і з зовнішніх запам’ятовуючих пристроїв;
- незаконне отримання паролів;
- розкриття шифрів криптозахисту інформації.

Розділ 1
§ 3

Загрози інформації за метою впливу

Відповідно до властивостей інформації, виділяють такі загрози її безпеки:

Загрози цілісності:	Загрози доступності:	Загрози конфіденційності:
▯ Модифікація (спотворення,) інформації; ▯ Заперечення дійсної інформації, ▯ Нав'язування фальшивої ;	▯ Блокування інформації; ▯ Знищення інформації та засобів її обробки;	▯ Несанкціонований доступ (НСД); ▯ Утрата (ненавмисна втрата, витік) інформації; ▯ Викрадення інформації, її розголошення.

Розділ 1
§ 3

Основні ненавмисні й навмисні штучні загрози

Загрози безпеці даних

Природні чинники	Старіння матеріалу носія	Розмагнічення, розшарування тощо
	Стихійні лиха	Пожежі, землетруси, блискавки тощо
Технічні чинники	Несправність обладнання	Перегорання, механічне пошкодження, збій у програмі тощо
	Зовнішній вплив	Перепади напруги, перегрів або переохолодження приміщення тощо
Людські чинники	Ненавмисні дії	Необережне поводження, помилки під час роботи з даними тощо
	Навмисні дії	Пошкодження вірусом, несанкціоноване використання тощо

Розділ 1
§ 3

Основні ненавмисні й навмисні штучні загрози

Шляхи поширення загроз (людський чинник)

Шляхи поширення загроз

- *Глобальна мережа Інтернет*
- *Локальна мережа*
- *Електронна пошта*
- *Знімні носії інформації*

Розділ 1
§ 3

Основні ненавмисні й навмисні штучні загрози

Загрози, які можуть завдати шкоди інформаційній безпеці організації, можна розділити на кілька категорій.

Загрози інформаційній безпеці

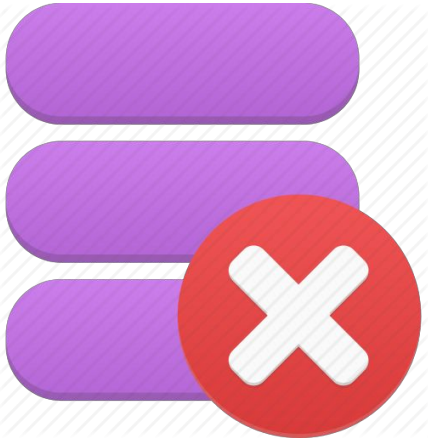
- *Дії авторизованих користувачів*
- *Дії хакерів*
- *Комп'ютерні віруси*
- *Спам*
- *Фішинг*
- *«Природні» загрози*

Розділ 1
§ 3

Які існують загрози безпеці та пошкодженню даних у комп'ютерних системах?

До категорії дій, що здійснюються авторизованими користувачами, належать:

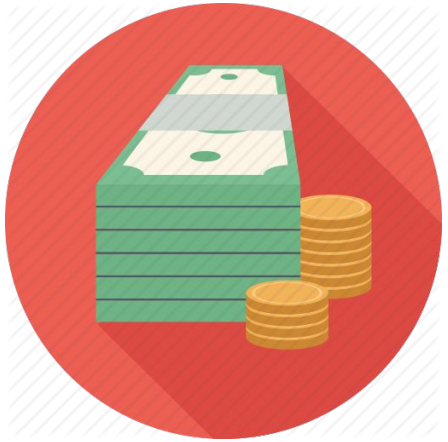
Цілеспрямована крадіжка	***Знищення даних на робочій станції або сервері***	***Пошкодження даних користувачами в результаті необережних дій***



Розділ 1
§ 3

Які існують загрози безпеці та пошкодженню даних у комп'ютерних системах?

Хакер *— кваліфікований ІТ-фахівець, який знається на роботі комп'ютерних систем і здійснює втручання до комп'ютера, щоб без відома власника дізнатися деякі особисті відомості або пошкодити дані, що зберігаються в комп'ютері. Їхні мотиви можуть бути різними:*

Помста	Самовираження	Винагорода
	*дехто робить це задля розваги, інші — щоб показати свою кваліфікацію*	

Цікаво

Напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена, називають DoS-атакою, або DDos-атакою.

(Англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack — атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні).

Розділ 1
§ 3

Запитання для рефлексії

1. *Що мені допомогло впоратися із завданням уроку?*
2. *Чи є в мене бажання ще більше дізнатися про ненавмисні й навмисні штучні загрози?*
3. *Чи було досягнуто особистої мети уроку?*
4. *Над чим мені слід попрацювати під час самоосвіти?*

Розділ 1
§ 3

Домашнє завдання

Зробити пост у соціальних мережах про навмисні штучні загрози інформації

Розділ 1
§ 3

Працюємо за комп’ютером

Створення буклета з рекомендаціями про навмисні штучні загрози інформації

1. *Відбір інформації для буклета*
2. *Пошук і відбір ілюстративного матеріалу для буклета*
3. *Розробка змісту буклета*
4. *Створення буклета засобами комп’ютерних технологій*
5. *Розповсюдження буклета в мережі Інтернет*

ІНФОРМАТИКА

Урок 3

Дякую за увагу!

За навчальною програмою 2018 року